IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEIZURE OF: ALL BITCOIN (BTC) VIRTUAL CURRENCY HOLDINGS STORED IN THE ACCOUNT ASSOCIATED WITH USER ID 69050519 AND E-MAIL ADDRESS rrg.btcxrp@gmail.com AT THE BINANCE CRYPTOCURRENCY EXCHANGE	**UNDER SEAL** Case No. 3:23-sw-105

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Michael J. McGillicuddy, after being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(c), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a seizure warrant. Specifically, I am a Special Agent with the Federal Bureau of Investigation ("FBI"), assigned to its Washington Field Office, Northern Virginia Resident Agency. I have been employed by the FBI for more than 17 years. From March 2015 through August 2016, I was a Supervisory Special Agent with the Money Laundering Unit at FBI Headquarters with oversight over the FBI's Money Laundering and Asset Forfeiture programs, among other threats. I am currently assigned to a squad, which has investigative responsibility for fraud-based and other economic crimes. I have participated in numerous criminal investigations to include violations related to corporate fraud, securities fraud, mail fraud, wire fraud, money laundering, and obstruction of justice. Prior to

joining the FBI, I was a forensic accountant for an economic consulting firm. I am a Certified Public Accountant and a Certified Fraud Examiner.

2. The facts in this affidavit come from my personal observations, my training and experience, review of records and documents, and information obtained from other law enforcement officials, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant. It does not set forth all my knowledge, or the knowledge of others, about this matter. The dates listed in the affidavit should be read as "on or about" dates.

PROPERTY TO BE SEIZED

3. This affidavit is made to obtain a seizure warrant for all Bitcoin ("BTC") virtual currency holdings ("**SUBJECT ASSETS**") stored in the account associated with User ID 69050519 and e-mail address rrg.btcxrp@gmail.com ("**SUBJECT ACCOUNT**") at the Binance cryptocurrency exchange ("Binance"). On April 4, 2023, Binance confirmed that it had put a voluntary freeze on the **SUBJECT ACCOUNT** pending a documented official request (i.e., seizure warrant or court order). As of April 4, 2023, the date Binance froze the **SUBJECT ACCOUNT**, a sum of 2.69196335 BTC remained in the **SUBJECT ACCOUNT**. BTC is volatile and subject to significant changes in value. As of April 16, 2023, one BTC was worth approximately $30,315.36. Accordingly, as of April 16, 2023, the value of the **SUBJECT ASSETS** in the **SUBJECT ACCOUNT** was approximately $81,607.84.

LEGAL AUTHORITY FOR SEIZURE

4. I have probable cause to believe that the **SUBJECT ASSETS** are subject to seizure and forfeiture because they are proceeds of, or traceable to proceeds of violations of 18

U.S.C. § 1343 (wire fraud) and are involved in a violation of both 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) and 18 U.S.C. § 1957 (unlawful monetary transactions), and therefore subject to civil forfeiture. Civil forfeiture authority is pursuant to 18 U.S.C. §§ 981(a)(1)(A) and 981(a)(1)(C).

5. 18 U.S.C. § 1343 (wire fraud) prohibits, in pertinent part, whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, from transmitting or causing to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

6. 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) prohibits, in pertinent part, whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, from conducting or attempting to conduct such financial transaction which in fact involves the proceeds of specified unlawful activity ("SUA") knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of SUA.

7. 18 U.S.C. § 1957 (unlawful monetary transactions) prohibits, in pertinent part, whoever, where the offense takes place in the United States ("U.S."), from knowingly engaging or attempting to engage in a monetary transaction in criminally derived property of a value greater than $10,000, which is derived from SUA.

8. 18 U.S.C. § 981(a)(1)(A) (civil forfeiture for violations of 18 U.S.C. §§ 1956 and 1957) provides for the forfeiture of any property, real or personal, involved in[1] a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 or 1957 as well as any property traceable to such property.

9. 18 U.S.C. § 981(a)(1)(C) (civil forfeiture for SUAs) provides for the forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to any offense constituting an SUA, as defined in 18 U.S.C. § 1956(c)(7), or a conspiracy to commit such SUA. 18 U.S.C. § 1956(c)(7)(A) provides that any act or activity constituting an offense under 18 U.S.C. § 1961(1) constitutes an SUA, with the exception of an act indictable under subchapter II of Chapter 53 of Title 31 of the U.S. Code. 18 U.S.C. § 1961(1) references violations of 18 U.S.C. § 1343.

10. 18 U.S.C. § 981(b)(2) provides that "[s]eizures pursuant to this section shall be made pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure…".

11. This Court has the authority to issue seizure warrants for assets located in another district and even outside the U.S. pursuant to 18 U.S.C. § 981(b)(3). Section 981(b)(3) provides that, "[n]otwithstanding the provisions of rule 41(a) of the Federal Rules of Criminal Procedure, a seizure warrant may be issued pursuant to this subsection by a judicial officer in any district in which a forfeiture action against the property may be filed under [28 U.S.C. § 1355(b)] and may be executed in any district in which the property is found, or transmitted to the central authority

[1] Assets "involved in" a laundering violation include the corpus of the offense, any funds laundered, any proceeds, and any property facilitating the offense. United States v. Miller, 295 F.Supp.3d 690, 697 (E.D.Va. 2018) (collecting cases), aff'd, 911 F.3d 229 (4th Cir. 2018).

of any foreign state for service in accordance with any treaty or other international agreement." 18 U.S.C. § 981(b)(3). Pursuant to 28 U.S.C. § 1355(b), a forfeiture action may be brought in any district court where any of the acts giving rise to the forfeiture occurred, even as to property located outside the district.[2]

BACKGROUND ON CRYPTOCURRENCY

12. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer ("P2P"), network-based medium of value or exchange that may be used as a substitute for fiat currency[3] to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are BTC, Litecoin, Ether ("ETH"), and Tether ("USDT").[4] Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is

[2] Binance is a cryptocurrency exchange registered in the Cayman Islands and, therefore, not subject to U.S. jurisdiction and cannot be compelled by U.S. process. However, as previously stated, Binance has placed a voluntary freeze on the **SUBJECT ASSETS** and is willing to turn them over to the U.S. with a seizure warrant issued by a U.S. Magistrate Judge.

[3] Fiat currency is currency issued and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

[4] USDT is a cryptocurrency "stablecoin" pegged to the U.S. Dollar (i.e., 1.0 USDT = approximately $1.00).

not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized P2P network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[5] Cryptocurrency is not illegal in the U.S.

b. BTC is a type of cryptocurrency. Payments or transfers of value made with BTC are recorded in the BTC blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire BTC through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), BTC kiosks (i.e., ATMs), or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" BTC by using his or her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. BTC transactions are therefore sometimes described as

[5] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

"pseudonymous," meaning that they are partially anonymous. And while it is not completely anonymous, BTC allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

c. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 26–36 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

d. Users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are

located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g., Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[6] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

e. BTC "exchangers" and "exchanges" are individuals or companies that exchange BTC for other currencies, including U.S. Dollars. According to Department of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[7] Such

[6] A QR code is a matrix barcode that is a machine-readable optical label.

[7] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guiadance/application-fincens-regulations-persons-administering.

exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions.

f. Although cryptocurrencies such as BTC have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering, and is an oft-used means of payment for illegal goods and services. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track transactions.

g. Based on my training and experience, I know that cryptocurrency can be laundered through multiple wallets and accounts in a manner that is similar to the laundering of fiat currency through different banks and bank accounts. However, with cryptocurrency this laundering has the potential to be done in a faster and more efficient manner than through banking institutions. Fraudsters attempt to obtain money from victims in the form of cryptocurrency because of its efficiency to be transferred from the U.S. and laundered through cryptocurrency accounts maintained by people and fraudsters outside of the U.S.

h. Based on my training and experience, I know that individuals engaged in criminal activity involving cryptocurrency frequently engage in "chain hopping," meaning that they convert funds from one cryptocurrency to another, often rapidly and in

quick succession, in order to obscure the source of funds and make it more difficult to track illicit funds as they move from one blockchain to another.

FACTS SUPPORTING PROBABLE CAUSE

Investigation Background

13. This investigation involves a fraud scheme that is currently fashionable and being perpetrated by multiple criminal groups, both domestically and internationally. The perpetrators use a variety of schemes to trick or coerce victims, many of whom are elderly, into providing them money. Initial contact with victims is typically made with automated, previously recorded telephone calls, commonly referred to as "robocalls," that contain misleading messages that often include callback numbers for victims to contact. Once contact is established, real people in the conspiracy will speak with the victims. One common technique used by the perpetrators is to offer the victims maintenance assistance with their home computers, convincing them that there are problems with their home computers, sometimes by tricking the victims into downloading software that the perpetrators use to actually create problems with the victims' computers. Another common technique is to offer the victims loans, purport that the loans were approved and the funds deposited, and require the victims to send money back as directed as a demonstration of good faith or as a loan payment.

14. With regard to many of the victims identified in this particular investigation, a more common scheme involved messages creating a sense of urgency by telling victims that they have some sort of serious legal problem, and that if they did not immediately take a particular action demanded by the callers then there would be drastic consequences, typically involving the arrest of the victims and/or significant financial penalties. The fraudsters almost invariably

instructed the victims that, in order to prevent these dire consequences, the victims must pay money, by wire transfer or cash, to some supposed government entity.

15. As a result of this investigation, between July 2020 and September 2022, 11 individuals who conspired to participate in the above-referenced schemes, which originated from several call centers in India, were convicted in the Richmond Division of this Court under case numbers 3:19-cr-160-HEH, 3:21-cr-47-HEH, 3:21-cr-48-HEH, 3:21-cr-49-HEH, 3:21-cr-70-HEH, and 3:22-cr-92-HEH.

VICTIM #1

16. On March 20, 2023, VICTIM #1, an 85-year-old male residing in Glen Allen, Virginia, received a pop-up notification on his laptop computer and subsequently called the provided telephone number, purportedly for "Microsoft." VICTIM #1 then provided the purported "Microsoft" technician with access to his computer. Upon scanning VICTIM #1's computer, the technician advised that certain funds in VICTIM#1's bank account had been withdrawn and sent to both Nigeria and Mexico. The technician stated that he could help VICTIM #1 prevent further losses by safeguarding VICTIM #1's money in a "seven layer secured account." The technician further advised that the FBI was working on VICTIM #1's case, the ultimate subject stealing VICTIM #1's money could be a bank employee or family member, and, as a result, VICTIM #1 should not tell anybody about VICTIM #1's work with the technician. Between March 20, 2023 and March 22, 2023, at the technician's direction, VICTIM #1 purchased $4,000 in Target-brand gift cards and provided the scratched off PIN numbers on the backs of the cards to the technician. On March 21, 2023, again at the technician's direction, VICTIM #1 made a cash deposit of $15,000 at a BTC kiosk located in or around Glen Allen. On

March 22, 2023, again at the technician's direction, VICTIM #1 made two additional cash deposits of $5,000 and $12,020, respectively, at BTC kiosks located in or around Glen Allen. The following day, on March 23, 2023, the technician provided VICTIM #1 with instructions for a $20,000 wire transfer to an individual residing in Thailand. While providing such instructions, VICTIM #1's daughter entered his apartment and overheard the end of his telephone call with the technician. VICTIM #1's daughter then immediately took him to his bank to freeze his accounts and then to the Henrico County Police Department to file a complaint. On March 31, 2023, VICTIM #1 subsequently filed a complaint with the FBI's Internet Crime Complaint Center ("IC3").

17. On March 31, 2023, at my request, VICTIM #1's daughter provided me with photographs of the receipts for the above-referenced cash deposits. I reviewed these receipts. They indicated that VICTIM #1's first deposit was for $15,000 in cash, resulting in 0.41166531 BTC (after fees) being deposited into BTC address bc1qamh8umh2hhceltzaa0frtgacqh8a3qnwx47gjp ("deposit address #1") on March 21, 2023. VICTIM #1's second deposit was for $5,000 in cash, resulting in 0.14280188 BTC (after fees) being deposited into BTC address bc1q3s939ups87uglgt6544lep2e00ufq5c82jz0cw ("deposit address #2") on March 22, 2023. Lastly, VICTIM #1's third deposit was for $12,020 in cash, resulting in 0.40208199 BTC (after fees) being deposited into BTC address bc1qzvu09prumpnsccevhx43d6e9ht0gs0sdk46kaq ("deposit address #3") on March 22, 2023.

18. On April 3, 2023, the 0.95654918 BTC of collective deposits described in the previous paragraph was further analyzed using BTC blockchain analysis tools. It was determined that, on March 22, 2023, deposit address #1 was one of six inputs to transaction hash

adf180c0c2dbff1f41642c120a9d7886a8eb933fc6cac815df2149f6208644f6, which sent 1.16809120 BTC to BTC address 1G622DY5UaisocbcayZ27daCVcCHubj4mn ("subject address"). On March 23, 2023, deposit address #2 was one of 11 inputs to transaction hash 6d7edfa0a904b3f4095bfe17b86181ff756fdbb94b449ceb5a9c83b9b7644c15, which sent 1.11263600 BTC to the subject address. BTC blockchain analysis further determined that the subject address was likely associated with Binance.

19. On April 3, 2023, in response to my request, Binance confirmed that the subject address was held by the **SUBJECT ACCOUNT** at Binance.

Binance Records

20. On April 3, 2023 and again on April 4, 2023, in response to my requests, Binance voluntarily produced information on the **SUBJECT ACCOUNT** that held the subject address. The owner of the **SUBJECT ACCOUNT** was listed as Sweety, a 55-year-old female residing in New Delhi, India. According to the **SUBJECT ACCOUNT**'s access logs, logins to the account on March 22, 2023 and March 23, 2023 utilized only two different IP addresses, both of which were geo-located in Delhi, India.

21. According to the **SUBJECT ACCOUNT**'s deposit history, the above-referenced deposit of 1.16809120 BTC (i.e., valued at approximately $31,905.25 at the time of the deposit) to the subject address, which included 0.41166531 BTC from VICTIM #1's first deposit, was the eighth most recent deposit into the **SUBJECT ACCOUNT**, posting at approximately 2:48 p.m. UTC on March 22, 2023. Approximately 2.5 hours later, at approximately 5:06 p.m. UTC, the **SUBJECT ACCOUNT** entered an order to sell the BTC and convert it to USDT. The following

day, on March 23, 2023, 48299.44725 USDT (i.e., valued at approximately $48,386.54 at the time of the withdrawal) was withdrawn from the **SUBJECT ACCOUNT**.

22. The above-referenced deposit of 1.11263600 BTC (i.e., valued at approximately $31,539.58 at the time of the deposit) to the subject address, which included 0.14280188 BTC from VICTIM #1's second deposit, was the seventh most recent deposit into the **SUBJECT ACCOUNT**, posting at approximately 6:24 p.m. UTC on March 23, 2023. Approximately 1.5 hours later, at approximately 7:55 p.m. UTC, the **SUBJECT ACCOUNT** entered an order to sell the BTC and convert it to USDT. Five days later, on March 28, 2023, 10445 USDT (i.e., valued at approximately $10,450.23 at the time of the withdrawal) was withdrawn from the **SUBJECT ACCOUNT**.

23. Subsequent to the above-referenced deposits, the subject address received six additional deposits totaling 8.91591146 BTC (i.e., valued at approximately $251,610.20 at the respective times of the deposits) in a very short period of time between March 28, 2023 and March 31, 2023. For three of the six deposits, orders were placed to sell the BTC and convert it to USDT within 30 minutes of the deposit.

24. On April 4, 2023, Binance confirmed that the **SUBJECT ACCOUNT** still maintained a balance of 2.69196335 BTC (i.e., valued at approximately $81,607.84 as of April 16, 2023). Based on my training and experience, given the eight different deposits totaling over 11.0 BTC (i.e., valued at over $315,000) that came into the **SUBJECT ACCOUNT** over the ten day period from March 22, 2023 to March 31, 2023, I believe the **SUBJECT ACCOUNT** is being used as a money laundering platform to launder the proceeds of the fraud committed against VICTIM #1 and other likely victims of Indian call centers.

Additional Reporting

25. In November 2021, Kraken, a cryptocurrency exchange based in San Francisco, California, reported alleged money laundering in three customer accounts which sent BTC valued at approximately $798,252.86 at the time to three different Binance BTC addresses, including the subject address. One of the Kraken accounts belonged to VICTIM #2, a 68-year-old male residing in Waco, Texas. VICTIM #2 told Kraken that his account was set up on his behalf after providing third-party access to his computer to a purported "Microsoft Security Team" technician.

26. In October 2022, Gemini, a cryptocurrency exchange based in New York, New York, reported elder financial exploitation related to the account of VICTIM #3, an 81-year-old female residing in Kennesaw, Georgia. In June 2022, VICTIM #3 deposited approximately $74,550 to her Gemini account via wire transfer. BTC and ETH valued at approximately $57,188.96 at the time was then transferred to four different Binance addresses, including the subject address.

CONCLUSION

27. Based on the foregoing, as well as my training, education, and experience, I submit that there is probable cause to believe that the **SUBJECT ASSETS** held in the **SUBJECT ACCOUNT** are not only proceeds of, or traceable to proceeds of violations of 18 U.S.C. §1343 (wire fraud) but also are involved in a violation of both 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) and 18 U.S.C. § 1957 (unlawful monetary transactions), and therefore subject to civil forfeiture pursuant to the authority set forth in paragraph 4 of this affidavit above. As previously stated, on April 4, 2023, Binance confirmed

that it had put a voluntary freeze on the **SUBJECT ACCOUNT** pending a documented official request (i.e., seizure warrant or court order).

Respectfully Submitted,

Date: 4/19/2023

Michael J. McGillicuddy
Special Agent
Federal Bureau of Investigation

Sworn to before and signed in my presence on this 19th day of April 2023, at Richmond, Virginia.

The Honorable Mark R. Colombell
UNITED STATES MAGISTRATE JUDGE